

Seven Design Requirements for Web 2.0 Threat Prevention

Secure Computing® is a global leader in Enterprise Security solutions. Powered by our TrustedSource™ technology, our award-winning portfolio of solutions help our customers create trusted environments inside and outside their organizations.

Table of Contents

Executive Summary	2
Introduction	2
Web 2.0 Defined.....	2
Web 2.0 Delivers Business Value.....	3
Obsolescence of NTP Caching.....	3
Web 2.0 Security Concerns.....	4
Inbound Threats	4
“But We Are Spending Billions Worldwide on Security!!!”	5
Outbound Threats	7
Solving the Web 2.0 Security Dilemma	7
Recommendations	7
The Solution: Seven Design Requirements for Web 2.0 Threat Prevention.....	8
Requirement #1: Deploy Real-Time Reputation-Based URL and Message Filtering for All Domains—Even Those Not Yet Categorized.....	8
Requirement #2: Deploy Anti-Malware Protection Utilizing Real-Time, Local “Intent-Based” Analysis of Code to Protect against Unknown Threats, as well as Signature-Based, Anti-Malware Protection for Known Threats	8
Requirement #3: Implement Bi-Directional Filtering and Application Control at the Gateway for All Web Traffic Including Web Protocols from HTTP to IM, Including Encrypted Traffic	9
Requirement #4: Data Leakage Protection on All Key and Web Messaging Protocols	9
Requirement #5: Ensure That All Caches and Proxies are “Security-Aware” for Safety and Efficiency Gains.....	10
Requirement #6: Design Security Infrastructure for Layering of Defenses with Minimal Number of Secure Devices	10
Requirement #7: Use Comprehensive Access, Management, and Reporting Tools.....	10
Secure Computing Products and Technologies for Web 2.0 Protection	11
Integrated Gateway Appliances.....	11
Secure Web (<i>Webwasher</i>) Solutions	11
Secure Mail (<i>IronMail</i>) Solutions	12

Secure Computing Corporation

Corporate Headquarters
 4810 Harwood Road
 San Jose, CA 95124 USA
 Tel +1.800.379.4944
 Tel +1.408.979.6100
 Fax +1.408.979.6501

European Headquarters
 Berkshire, UK
 Tel +44.(0).1344.312.600

Asia/Pac Headquarters
 Wan Chai, Hong Kong
 Tel +852.2598.9280

Japan Headquarters
 Tokyo, Japan
 Tel +81.3.5339.6310

For a complete listing of all our global offices, see www.securecomputing.com/goto/globaloffices

Executive Summary

The rapid adoption of Web 2.0 applications has opened up the enterprise to new security threats that are not stopped by the widely deployed Web and messaging security solutions currently in place. Addressing Web 2.0 threats requires a new generation of multi-layered security that builds on traditional security protocols with both inbound and outbound protection, reputation-based filtering, and multi-function security appliances at the network gateway. A recently completed commissioned study conducted by Forrester Consulting on behalf of Secure Computing entitled *Internet Risk Management in the Web 2.0 World* shows that while Web 2.0 threats are real and enterprises are aware of them, they have not taken sufficient action to protect themselves.¹

Drawing on customer experience, Forrester Consulting, and data gathered from TrustedSource™ technology (the Secure Computing® global Web and messaging reputation system), as well as third-party sources, this paper outlines the new Web 2.0 threats and explains why most security solutions in place today are not adequate to protect against these threats. The paper then goes on to propose a set of **Seven Design Requirements for Web 2.0 Threat Prevention**, and reviews Secure Computing's relevant product and technology offerings.

Introduction

The Internet today is a different place than it once was. Widely referred to as "Web 2.0," today's Internet has and will continue to evolve as innovators use new Web technologies to implement new applications. However, this innovation is usually done with security as an afterthought; and end-user adoption of Web 2.0 is simply outpacing the implementation of adequate security solutions.

Applications are now Internet-enabled and the use of corporate intranets and extranets have become critical components of business. Indeed, organizations now build their businesses on Web infrastructures, and mainstream organizations are already using Web 2.0 technologies both internally and externally. Today's business model relies on the Web to provide inbound access for remote employees, partners, and customers from any location, anywhere in the world. Internal employees also reach beyond the edge of the internal network to communicate and gather information across the Internet. These innovations have brought businesses great efficiencies, and have enabled companies to expand their sphere of influence globally at low cost. However, when you add the rich browser-based, bi-directional aspect of Web 2.0 applications, even more risk is introduced into the enterprise. Communication methods are both inbound and outbound, and so too, are the related threats. At the same time that Web 2.0 has become an integral part of any legitimate business, so too has it become an integral part of criminal enterprise.

The enterprise must be protected from malware (malicious software), regulatory compliance must be ensured, data leakage prevented, and employee productivity must be managed. These security issues exist for all IP-based traffic, whether email, VoIP, instant messaging, Web access, file transfers, or other enterprise applications communicating over IP.

In short, user and business use of the Web and its related applications exposes organizations to both inbound and outbound security threats which transcend the legacy security measures for Web 1.0. The new generation of emerging security threats now consists of malicious attacks led by highly organized cyber-criminals with sophisticated tools targeted at specific organizations for personal or financial gain. This paper outlines these new threats and discusses the limited effectiveness of legacy Web security solutions against those threats. The paper then outlines the new proactive security paradigm that is necessary for securing Web 2.0 applications and protecting the enterprises that use them on a daily basis.

Web 2.0 Defined

Let's begin by looking at what "Web 2.0" is.

The original concept of Web 2.0 has been credited to Tim O'Reilly and MediaLive International and was said to be the result of a brainstorming session that resulted in the first *Web 2.0 conference*. On May 16, 2006 the United States Patent and Trademark Office (USPTO) began allowing them to trademark the term Web 2.0 for use in their conferences.

¹ Forrester commissioning study *Internet Risk Management in the Web 2.0 World*.

A true, definitive version of Web 2.0 is hard to pin down, and in fact, a static definition is impossible to create because of the dynamic nature of Web 2.0. In the initial brainstorming session of Tom O'Reilly and MediaLive International, they formulated a sense of Web 2.0 by example:

DoubleClick	⇒	Google AdSense
Ofoto	⇒	Flickr
Akamai	⇒	BitTorrent
mp3.com	⇒	Napster
Britannica Online	⇒	Wikipedia
personal Websites	⇒	blogging
evite	⇒	upcoming.org and EVDB
domain name speculation	⇒	search engine optimization
page view	⇒	cost per click
screen scraping	⇒	Web services
publishing	⇒	participation
content management systems	⇒	wikis
directories (taxonomy)	⇒	tagging ("folksonomy")
stickiness	⇒	syndication

<http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-Web-20.html>

The original *Web 2.0 article* written in 2005 by Tim O'Reilly provides his highly regarded definition of Web 2.0.

Wikipedia, itself a *Web 2.0* collaborative application, provides this additional definition:

"In alluding to the *version*-numbers that commonly designate software upgrades, the phrase "Web 2.0" hints at an improved form of the World Wide Web. Technologies such as *Weblogs*, *social bookmarking*, *wikis*, *podcasts*, *RSS feeds* (and other forms of many-to-many publishing), *social software*, *Web application programming interfaces* (APIs), and online *Web services* such as *eBay* and *Gmail* provide a significant enhancement over read-only Web sites. *Stephen Fry* (actor, author and broadcaster) describes Web 2.0 as "an idea in people's heads rather than a reality. It's actually an idea that the reciprocity between the user and the provider is what's emphasized. In other words, genuine interactivity if you like, simply because people can upload as well as download." The phrase "Web 2.0" can also refer to the transition of *Web sites* from isolated *information silos* to interlinked *computing platforms* that act like software to the user. Web 2.0 also includes a social element where users generate and distribute content, often with freedom to share and re-use. The result is a rise in the economic value of the Web as users can do more online."

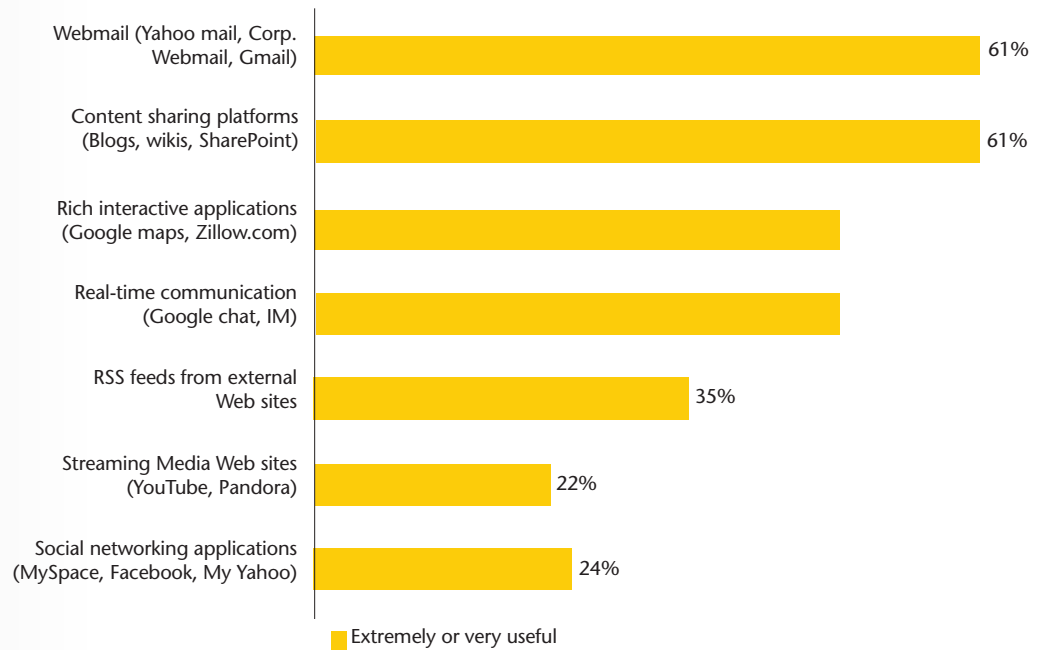
Web 2.0 Delivers Business Value

Some of the most popular Web 2.0 applications are consumer-focused, and include things like music and video sharing Web sites, and social networking, some of which employees may attempt to use on work equipment. In addition, Web 2.0 applications deliver business value and are here to stay. Secure Computing's recently commissioned study by Forrester Consulting confirms this fact, showing that numerous Web 2.0 applications are useful for business purposes. The study shows that 90% of organizations rate one or more Web 2.0 type applications as extremely or very useful for its enterprise:

Obsolescence of NTP Caching

At one point news groups even had caching created for them. The rapid adoption of Web 2.0 blogs (which use HTTP) and user forums have made news groups (and the need for news group NTP caching) obsolete.

Figure 1: "Please rate the usefulness of each category of Web 2.0 application for your organization"*



Base: 153 senior IT and security professionals

*Some percentages do not total 100 due to rounding

Source: A commissioned study conducted by Forrester Consulting on behalf of Secure Computing

But what about the security that is essential in protecting the enterprise from the threats created by the broad adoption of these Web 2.0 applications?

Web 2.0 Security Concerns

Inbound Threats

The press is full of examples of examples of Web 2.0 security threats such as the Monster.com data breach² and the Yahoo XSS error (that enabled malware to steal user passwords³). Hacking tools continue to be developed to help create sophisticated malware⁴. Many of these malicious tools are widely available on the Internet at low cost, and are developed with easy graphical "point and click" interfaces so that even unskilled users can use them to break into your computer and steal your information.

Many of these threats are greatly refined and not only use the Web (HTTP) but also encrypted (HTTPS) and email (SMTP) protocols to pull off their attack. As an example, autumn of 2006 leveraging of the Web 2.0 site Wikipedia⁵ with spam and a third party Web site links illustrates the need to provide threat protection that takes into account the use of multiple protocols. In this attack "Malware writers... used a Wikipedia article to lead users to a booby-trapped page that contained malicious code designed to plant viruses on the computers of unsuspecting users. The hackers created a Wikipedia page that offered a Windows security update for a version of the Lovesan/W32.Blaster worm, and included a link to an external site that was labeled with the name 'wikipedia-download.org'...The attackers directed users to those archived pages through emails that used the Wikipedia logo, and claimed that the encyclopedia site had been asked by Microsoft to help with worm patches."

The publicity around such attacks has not gone unnoticed. Enterprise security management is aware of the security risks inherent in the adoption of Web 2.0 technologies and applications. The same Forrester study (see Figure 2) showed that businesses are wary of Web 2.0 usage and of the ensuing threats. Ninety percent of organizations are extremely or very concerned about specific threats from Web 2.0

² http://www.usatoday.com/tech/news/coomputersecurity/infotheft/2007-08-23-cyberjobs_n.htm

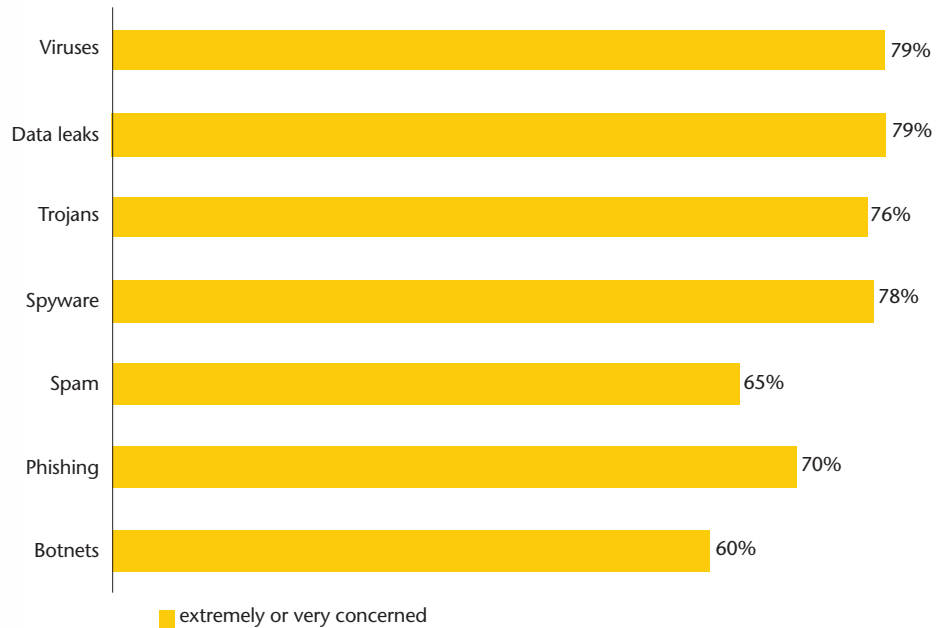
³ http://www.theregister.co.uk/2007/06/15/yahoo_xss_error/

⁴ http://www.pcworld.com/businesscenter/article/127542/hackers_projects_hides_browserbusting_code.html

⁵ http://www.toptechnews.com/story.xhtml?story_id=101003HCTOK6

applications. Yet according to Secure Computing’s calculations, less than 5% have adequate Web Gateway protection. In addition, new threats are possibly being overlooked, as only 60% of respondents in the survey were extremely or very concerned about “botnets,” yet over one million computers are now part of the Storm botnet!⁶

Figure 2: “How concerned are you about each threat, which may be brought on by Web 2.0?”*



Base: 153 senior IT and security professionals

*Some percentages do not total 100 due to rounding

Source: A commissioned study conducted by Forrester Consulting on behalf of Secure Computing

“But We Are Spending Billions Worldwide on Security!!!”

Over time, we have addressed the majority of security issues with the underlying protocols for Web 1.0. And organizations have deployed solutions like signature-based antivirus to address those issues. Those signature-based solutions became very effective in combating early Web 1.0 threats. Yet the attacks continue and security management is rightfully concerned.

Today’s layering of new next-generation programming languages on top of these protocols in Web 2.0 has given those with malicious intent a whole new set of technologies to exploit. Signature-based solutions and other Web 1.0 security practices continue to be a necessary part of the security infrastructure, but by themselves, these security practices are no longer enough. A great example of this would be AJAX, the popular Web 2.0 programming language. The asynchronous nature of AJAX clearly improves the users’ experience on a Web site by taking interactivity to an entirely new level. However, it also dramatically increases the chances that things can go terribly wrong from a security perspective.

One tactic used by these cyber-criminals is to leverage their sophisticated knowledge to plant worms on host machines. These compromised machines, known as zombies, are rented out to carry out phishing, spam or other attacks.⁷

In addition to for-hire zombie networks (“botnets”) cyber-criminals also use sophisticated tools to deploy seemingly innocent content which actually contains Trojan horses with malicious functions. These targeted Trojan horses present a threat to the organization in that on the surface, they appear harmless and innocuous, and may even take the form of a useful application or an entertaining game. Often these attacks utilize common productivity tools like MS Office files transmitted via work email or via personal email that employees access via encrypted Web mail. Once opened by the recipient, the Trojan is released, opening the door for corporate data espionage, data theft, and the release of

⁶ TrustedSource.org

⁷ http://news.com/com/2102-7349_3-5772238.html?tag=st.util.print

additional malware. **Traditional anti-virus solutions are ineffective in stopping the attack because there is no known signature.** Targeted attacks are increasingly brief in duration and small in number of samples sent out. Often it consists of malware that is designed to by-pass the targeted company's signature-based anti-virus protection. Since the attack can end in just a few hours, your data may have already been stolen before anyone knows it has happened.^{8,9}

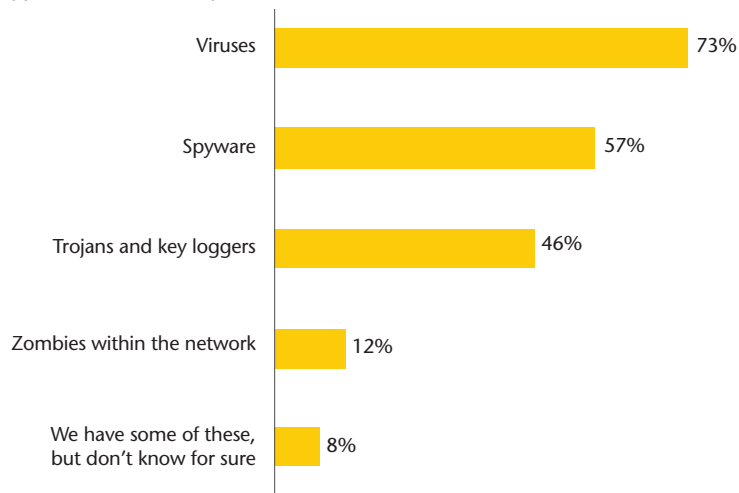
And it is not just files coming into an organization hidden in Trojans that can introduce malware. Seemingly innocent Web pages that employees may access for legitimate purposes can introduce malware or spyware into a network. This is potentially much more dangerous. Users can be educated not to click on suspicious email attachments, but malicious Web sites may contain active code that launches automatically as soon as the Web page is viewed. Can we teach an end user what sites are trustworthy and which are not? Unfortunately we can't.

One example of how signature-based anti-virus protection and category-based URL filtering have become obsolete due to the dynamic nature of Web 2.0 threats, is a program now available called "eVade o'Matic Module," or VOMM for short, that automates the creation and modification of code so that it **constantly changes its signature to avoid anti-virus detection while taking advantage of the same browser vulnerability.** VOMM enables malicious code to literally have an infinite number of possible signatures, so that the malware can always stay a step ahead of the anti-virus software. In short, its purpose is to make an intrusion attempt undetectable by signature-based anti-virus protection.¹⁰

Malicious attacks are also now utilizing the very technologies that were created to provide security. For example, to secure financial transactions, encrypted HTTP was created (HTTPS) to ensure that financial data was not "in the clear" on the Internet. However, attackers can also use this secure connection to transmit malware, and carry out a malicious attack that is undetectable by legacy security solutions like anti-virus.¹¹ Because most legacy security solutions cannot be applied to encrypted traffic, we refer to this portion of network traffic as the "SSL blind spot."

Is it any wonder then, that worldwide, organizations collectively spend billions each year on security software, especially signature-based anti-virus solutions, yet organizations are not adequately protected? The Forrester study shows that these solutions are not completely effective in protecting the enterprise from infection:

Figure 3: "What type of infection have you had in the last 12 months?"



Base: 153 senior IT and security professionals (multiple selections accepted)
 Source: A commissioned study conducted by Forrester Consulting on behalf of Secure Computing

⁸ http://news.com.com/2102-7349_3-6125453.html?tag=st.util.print

⁹ <http://www.itpro.co.uk/security/news/99467/2006-the-year-of-targeted-malware.html>

¹⁰ <http://www.itsecurity.com/features/news-feature-metasploit-vomm-102906/>

¹¹ <http://www.windowsecurity.com/whitepaper/info/misc/tricks.html>

The study found that 97% of respondents reported themselves as prepared or extremely prepared to deal with Web 2.0 threats, yet 79% of enterprises have reported more than infrequent occurrences of malware infections. In addition, the study showed companies spent anywhere from \$15 to \$30 per user, per year on direct malware clean-up costs. This year, Computer Economics estimated that these costs were over \$13B globally.¹² And these numbers do not take into account the indirect costs of lost productivity and reputation which, no doubt, are many times this number.

The Forrester study further notes:

“The type of malware that makes past the Web filtering gateway is most likely of the “zero-day” variety, as otherwise it would have been caught by URL filtering or signature scanning. Signature scanning cannot detect zero-day attacks as by definition there are no “signatures” available for zero-day threats. The only hope to catch zero-day attacks is to employ “on-the-fly,” dynamic detection capabilities such as behavioral and heuristics based detection. Without that, many attacks will go undetected.”

Outbound Threats

In addition to inbound threats, there are also outbound data leakage threats that jeopardize critical and sensitive information vital to an organization’s success. Attackers aren’t always outsiders in faraway countries; more often they are right inside your own organization. Data thieves, industrial spies, and cyber-vandals can, and often do, operate within a company’s own boundaries. But outbound threats aren’t always the result of an intentional attack by an insider; sometimes they occur when an employee unintentionally opens or allows a “back door” to be opened by downloading a rogue application that has not been approved by IT.

Outbound data leakage is a concern for two reasons: 1) risk of intellectual property loss and 2) compliance with regulatory and/or industry requirements (e.g. SOX, HIPAA, GLBA, PCI, etc.). Many organizations think that filtering their email is sufficient to provide protection. While doing so is a key factor in a leakage prevention strategy, a multi-protocol approach to data leakage security, where network security administrators also pay attention to Web protocols as well is best. Rapid adoption of blogs, wikis, employee access to personal email (which is sometimes encrypted) via the Web are all potential data leakage points for the enterprise. As a result Web (HTTP), encrypted Web (HTTPS), instant messaging (IM), and file transfers (FTP) are all potential data leakage methodologies because all of these protocols can be used to convey proprietary information out of the enterprise.

Solving the Web 2.0 Security Dilemma

We have demonstrated that deployment of legacy category-only Web filtering and signature-based anti-virus are not adequate to protect against Web 2.0 threats and the Forrester study shows that organizations widely recognize this. What should organizations do to provide security in our rapidly evolving Web 2.0 world?

Recommendations

The Forrester study makes the following recommendations:

- Re-examine the adequacy of security policies and protection capabilities
- Improve user awareness and training on Web 2.0 and Web-borne threats;
- Deploy next-generation proactive protection
- Deploy solutions that deliver enterprise-level performance, scalability, and manageability support

¹² “2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other Malicious Code,” Computer Economics

The Solution: Seven Design Requirements for Web 2.0 Threat Prevention

Forrester's recommendations include product and technology investments in next-generation proactive protection. To achieve this, Secure Computing recommends implementing *Seven Design Requirements for Web 2.0 Threat Prevention*:

1. Deploy proactive real-time reputation-based URL and message filtering for all domains—even those not yet categorized
2. Deploy anti-malware protection utilizing real-time, local “intent-based” analysis of code to protect against unknown threats, as well as signature-based, anti-malware protection for known threats
3. Implement bi-directional filtering and application control at the gateway for all Web traffic including Web protocols from HTTP to IM, including encrypted traffic
4. Monitor for, and protect against, data leakage on all key Web and messaging protocols
5. Ensure that when deployed, all proxies and caches are fully security-aware
6. Design layered defenses with minimal number of proven and secured devices
7. Use robust management and audit reporting tools for all Web and messaging protocols, services and solutions including filtering, malware, and caching.

Requirement #1: Deploy Real-Time Reputation-Based URL and Message Filtering for All Domains—Even Those Not Yet Categorized

Just as legacy anti-virus solutions that utilize signatures are not adequate to stop malware, legacy URL filtering solutions are also insufficient. They rely only on categorized databases of URL entries that only update a few times a day. What is needed is a “reputation system” that assigns global reputations to URLs and IP addresses, and works alongside the categorized databases for the ultimate protection.

A sophisticated, third-generation reputation system provides a mechanism for determining the risk associated with receiving data from a particular Web site. This reputation can be used in conjunction with categories in an organization's security policy, allowing them the ability to make the appropriate decision based on both category and security reputation information. This reputation-based URL filtering solution needs to be global in scope and internationalized to handle Web sites in any language.

It is critical that the reputation system provide both Web and messaging reputation. Since malicious attacks are multi-protocol, the reputation system must be aware of both email and Web threats. A new domain without content cannot be categorized, but if it is associated with IP addresses sending email and they have a history of SPAM, phishing or other malicious activity, then the Web reputation for this uncategorized domain can immediately be determined and security protection provided to those who try to access it.

Organizations should deploy email gateways that utilize sender reputation to stop malicious attacks, often launched via spam and social engineering. Email reputation is also critical as spam, phishing and other malicious emails will include an URL or IP address that needs to be immediately fed back into the Web gateway security infrastructure.

Requirement #2: Deploy Anti-Malware Protection Utilizing Real-Time, Local “Intent-Based” Analysis of Code to Protect against Unknown Threats, as well as Signature-Based, Anti-Malware Protection for Known Threats

Enterprises should deploy intent-based anti-malware at both the Web and email gateway. These solutions include a signature-based antivirus engine to stop known threats but, more importantly, address the problem illustrated in the Forrester study:

“Realigning your security policies with risk initiatives would call for shifting malware protection to be the No. 1 priority. This should result in the subsequent deployment of Web-filtering capabilities beyond URL filtering and signature scanning. More specifically, protection against Web-borne malware should include Web site reputations, real-time behavioral analysis, and heuristics-based detection that allows for more thorough content inspection and detection of zero-day threats.”

These malware solutions utilize “intent-based” analysis to examine code at the gateway entering via email attachment or mobile code that will execute in the browser. Malware protection should:

- Perform a “magicbyte” analysis of each file to determine the actual file type
- Safeguard against files that are disguised to be something they are not
- Disallow media types that are potentially hazardous (like unknown ActiveX)
- Check active code for valid digital signatures
- Execute behavioral analysis to determine if it will behave in a known manner
- Analyze scripts to determine if they are trying to exploit vulnerabilities on the client
- Neutralize attacks as needed

Most important is notifying a global reputation system whenever any Web or email gateway finds malware for which no signature exists. This is critical to participation in the reputation ecosystem. Whenever malware is found on a Web page or in an email, the reputation system is notified so that reputation for that domain or IP can be immediately updated so that all organizations participating in the reputation ecosystem have immediate benefit.

For more information on how to stop malware please see our *Stopping the Targeted Attack* white paper.¹³

Requirement #3: Implement Bi-Directional Filtering and Application Control at the Gateway for All Web Traffic Including Web Protocols from HTTP to IM, Including Encrypted Traffic

Applications that communicate over encrypted and unencrypted protocols need to be controlled in both directions. This includes controlled access to these applications (Web sites, blogs, wikis, IM, P2P, etc.) as well as monitoring the connections for malware coming in and data leakage going out. With the high percentages of corporate Web traffic now encrypted (HTTPS) it is imperative to be able to selectively decrypt this content at the gateway to provide security while respecting privacy for access to sensitive sites such as personal finance sites.

Requirement #4: Data Leakage Protection on All Key and Web Messaging Protocols

Providing data leakage protection on all outbound content via either Web or email is a four-step process. From defining corporate and regulatory policies to detecting and enforcing them, to proving compliance to auditors, this process is the surest way to ensure that no inappropriate information ever leaves your gateway.

The four steps to achieve compliance are:

Policy Definition - knowing what should be done and by whom

Violation Detection - determining the actual content in a message and whether or not it constitutes “sensitive information” that needs to be protected

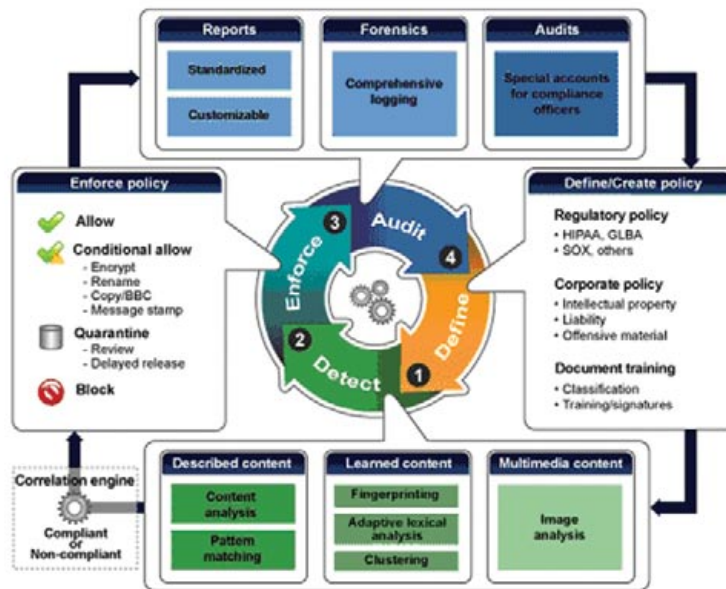
Automatic Enforcement - applying the appropriate security measures based on content and senders

Reporting and Auditing - proving what happened

Data leakage protection needs to be provided over encrypted and unencrypted protocols for both messaging and Web traffic. This includes controlled access to these applications (Web sites, blogs, wikis, IM, P2P, etc.) as well as monitoring the connections for data leakage. With the high percentages of corporate Web traffic now encrypted (HTTPS) it is imperative to be able to selectively decrypt this content at the gateway to provide security while respecting privacy for access to sensitive sites such as personal finance sites.

¹³ <http://www.securecomputing.com/Webform.cfm?id=81&sourcecode=wgsw>

Figure 4: Data leakage requirements



Requirement #5: Ensure That All Caches and Proxies are “Security-Aware” for Safety and Efficiency Gains

Objects that are cacheable must be filtered for malware, security reputation, and URL filtering policy prior to delivery to the requestor’s browser. Cached objects must have these filters applied each time the object is delivered to the end user because the reputation may have changed since the object was originally cached or the security policy of this requestor may be different than the previous requestors. This policy might be different in any of these areas: security reputation, URL filter policy or malware. Deploying caches and proxies that are not security aware runs the risk of delivering malicious code to the user.

Requirement #6: Design Security Infrastructure for Layering of Defenses with Minimal Number of Secure Devices

Gateway security today provides for a robust point of policy definition, enforcement and monitoring. Given the use of gateway’s as security enforcement points, it is important to ensure that the devices are secure, and provide layering of defense within the device, as well as in concert with other devices as well as endpoint security. As we have seen, today’s most effective defense combines signature bases, reputation based AND intent based defenses, working together. In addition devices must not create additional “blind spots” such as SSL traffic, or introduce new vulnerabilities themselves. To manage risk cost effectively, for example, today’s Web gateway requirement is for a single solution approach that houses the security engine and caching engine in the same application, tightly integrated, sharing the same memory and—above all—on the same appliance. In addition to having fewer vendors to deal with, replacing point solutions with multifunction integrated appliances that provide best of breed functionality has the benefits of added protection, since the cache can be security-aware malware can be integrated with Web filtering reputation, etc. In addition, on protocols such as Web and SMTP, effective outbound protection can now be as important as inbound protection. Solutions which manage both inbound and outbound risk, reduce costs and increase security by providing for additional opportunities for consolidation and efficiency.

Requirement #7: Use Comprehensive Access, Management, and Reporting Tools

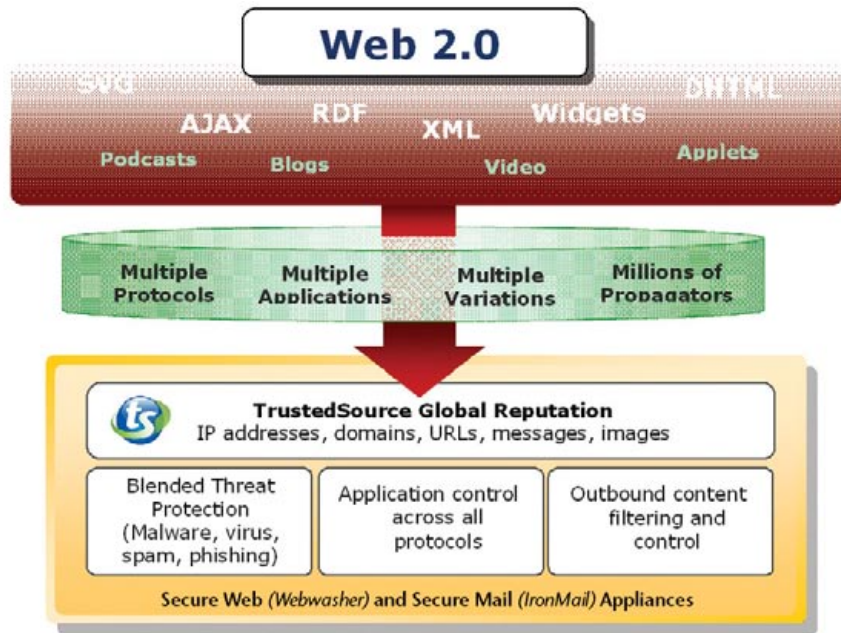
Enterprises should deploy solutions that provide “at-a-glance” reporting on the status and health of their email and Web gateways. They also need both real-time and forensic reporting that allows them to drill down into problems for remediation and post-event analysis. Providing robust and extensible reporting is a critical function to understand risk, refine policy, and measure compliance.

By deploying solutions that meet most if not all of these requirements, IT security teams can move beyond their legacy Web 1.0 and messaging security infrastructure and deliver protection that better aligns with risk based on today’s threat environment. Not doing so is akin to living in a fault zone in a brick mud house; it is not a matter of if, but when the risks will catch up with you.

Secure Computing Products and Technologies for Web 2.0 Protection

Building on these principles, Secure Computing is actively investing in its Web gateway security solution, Secure Web (*Webwasher*), and its Email gateway security solution, Secure Mail (*IronMail*), to provide the industry's most complete protection against threats from Web 2.0 and beyond. Secure Computing positioned in the Leaders Quadrant of Gartner's Web Gateway Magic Quadrant and as a Top Player in Radicati Group's Email Security Appliance Market Quadrant.¹⁴ In addition, we continue to invest in our 3 core technologies to manage Web 2.0 risk, TrustedSource, our global reputation system that provides security to all customers on the TrustedSource network, as well as our award-winning and market-leading anti-malware and outbound compliance engines.

Figure 5: Secure Computing Products and Technologies for Web 2.0 Protection



Integrated Gateway Appliances

Secure Web (*Webwasher*) Solutions

Secure Web (*Webwasher*) appliances protect enterprises from malware, data leakage, and Internet misuse, while ensuring policy enforcement, regulatory compliance and a productive application environment. Secure Web analyzes traffic bi-directionally. Inbound, it isolates and eliminates threats from all types of malware—zero-day threats, viruses, Trojans, spam, phishing, and the like. Secure Web employs the most sophisticated intent and signature-based techniques for stopping malware and zero-day attacks, as well as patented content analysis software to achieve regulatory compliance and for stopping data leakage on outbound traffic. Secure Web uses a deep knowledge of the underlying protocols and application behavior combined with global intelligence to make security decisions.

Secure Web (*Webwasher*) is a truly integrated solution that replaces legacy point solutions. Secure Web has a unified interface that combines all the content protection applications enterprises need into one solution: reputation-based Secure Web Filter, Anti-Malware (with anti-virus signatures), SSL scanning, Secure Web Cache next-generation security cache, anti-spyware, and enterprise-level reporting on all Web traffic. Secure Web integrates with Secure Computing's Secure Mail (*IronMail*) solution for email protection. Integration between the Secure Web and Secure Mail solution is critical since many of today's attacks utilize multiple modes. The attack may begin with a seemingly innocent email with an embedded URL that, when accessed by the recipient, launches a Web-based attack.

¹⁴ Gartner, Inc., *Magic Quadrant for Secure Web Gateway, 2007*. Peter Firstbrook, Lawrence Orans, Arabella Hallawell, 4 June 2007. Radicati Group, Inc., *Email Security Appliances - 2007 Market Quadrant*, Matt Anderson, Sara Radicati, August 2007.

Traditional URL filtering solutions stop users from visiting certain sites that cause liability risks, loss of productivity, or sap bandwidth, but do very little to protect against compromised legitimate Web sites. Secure Computing has defined a new standard in URL filtering with its integration of the TrustedSource reputation technology with each of the millions of URLs in its award-winning Secure Web SmartFilter database, now used to power Secure Web Filter. Instead of relying solely on a static list of categorized URLs, Secure Web enhances protection by adding “Internet reputation” to what is known about the URL and enables a ‘block or allow’ decision based on real-time information. The ability to implement security policy based on both URL category and its Web reputation dramatically improves filtering accuracy and protection. Whenever a Secure Web gateway finds malware in a Web page by virtue of the anti-malware protection, that threat is not only stopped at the gateway but reported back to Secure Computing via TrustedSource in real time, providing intelligence and protection to all of Secure’s customers.

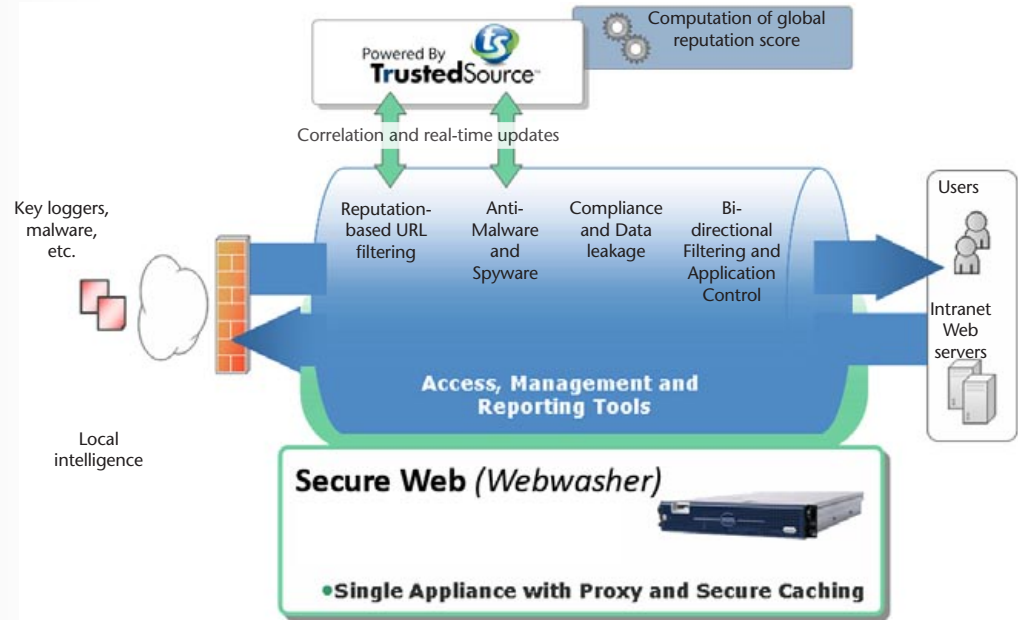


Figure 6: Secure Web (*Webwasher*) Solution: Protection from Web 2.0 Threats

Secure Mail (*IronMail*) Solutions

Secure Mail (*IronMail*), the flagship product of the Secure Mail portfolio, is the world’s leading email security appliance, having placed in the Top Players’ quadrant by Radicati Group. It is a five-star “Best Buy” from SC Magazine and the winner of the “Best of the Best” from Search Security.

Secure Mail is about blocking the bad and guarding the good. It’s a unique combination of:

- Global and local protection to provide maximum effectiveness
- Multiple-protocol protection to provide maximum coverage
- Custom-built appliance protection to provide maximum ROI
- Best-of-breed inbound plus outbound protection to provide maximum enforcement

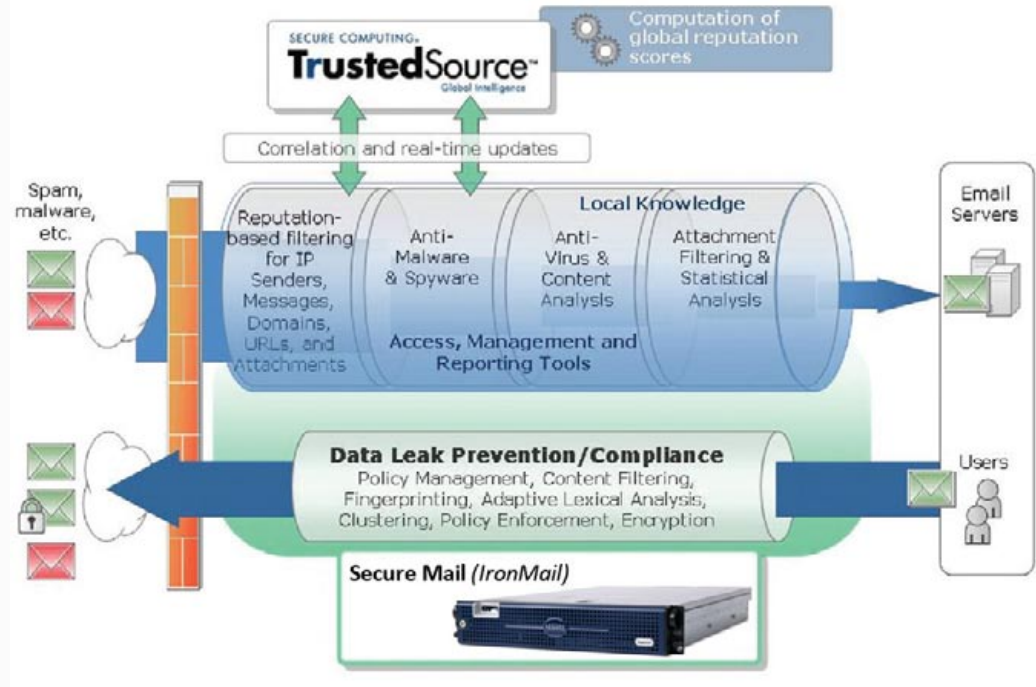
Secure Computing’s Secure Mail solutions are unique:

- Deliver constant and ongoing optimal security, rather than a temporary window of protection
- Prevent direct attacks as well as attacks on the email infrastructure
- Provide proven protections, tested every day in the most demanding environments in the world, including:
 - o Enterprises of every size and industry
 - o Government agencies worldwide

- o Educational institutions
- Apply consistent policy enforcements against multiple messaging protocols
- Protect outbound content as securely as inbound messages

This complete family of application-specific, bi-directional messaging security and compliance appliances fully leverages the global intelligence of TrustedSource. They are designed to perform at enterprise-speeds, scale to meet global requirements, and can be deployed and managed with minimal overhead.

Figure 7: Secure Mail (IronMail) Email Gateway Security



Secure Computing Technologies

To support these security products, Secure Computing has invested extensive time and resources in the underlying technologies that can create this strong security model. The first, and most important, is TrustedSource, our global reputation service.

TrustedSource

From its early days of simply assigning reputations to IP senders, TrustedSource now provides more reputations, with more granularity, than any other reputation service available. TrustedSource assigns reputations to:

- IP Senders
- Messages
- Attachments and images
- URLs
- Domains

Secure Computing developed TrustedSource to keep enterprises ahead of the spammers in the ongoing battle for the inbox. TrustedSource gathers information on email senders and the types of email they generate by accumulating data from thousands of sensors located



in 72 countries. Since TrustedSource sees over 110 billion messages a month—more than any other messaging security technology—it can provide superior accuracy when creating a reputation score. Relying on this score, TrustedSource can block up to 80% of connections based purely on reputation data (over 6.2 terabytes of spam every day), increasing security levels while maintaining a false positive rate of less than one in one million.

But spam is only one threat in today’s Web 2.0 world. Since its inception, TrustedSource has been expanded to protect against all forms of attacks, both known and unknown, via either the Web or email.

As part of Secure Computing’s vision to provide comprehensive enterprise gateway security, Secure Web (*Webwasher*) now incorporates global intelligence from TrustedSource. TrustedSource provides real-time reputation scores for URLs, domains, and IPs based on Web page content, images and behavior. TrustedSource also considers historical information such as knowledge that a site has been repeatedly compromised in the recent past. Using this real-time scoring, Secure Web allows organizations to detect and prevent security threats such as spyware, phishing, or other malware.

Anti-Malware Engine

Secure Computing’s Secure Web Anti-Malware engine is a next-generation approach to protecting the network from malware. Secure Computing’s Anti-Malware engine has been rated #1 by AV-test.org, an independent research center.¹⁵

Secure Computing’s Secure Web Anti-Malware engine contains a signature-based anti-virus engine to protect against known threats as well as a proactive behavioral analysis engine that analyzes mobile code at the gateway (before it reaches the desktop) to determine its intent should it be allowed to reach the desktop. It is the effectiveness of this intent analysis that results in the Secure Computing’s Anti-Malware engine to consistently deliver number one ratings in independent tests.

For a detailed discussion of how Secure Computing’s Anti-Malware engine protects the Web gateway, please see our whitepaper.¹⁶

Figure 9: Summary of AV-Test.org test results from May 2007

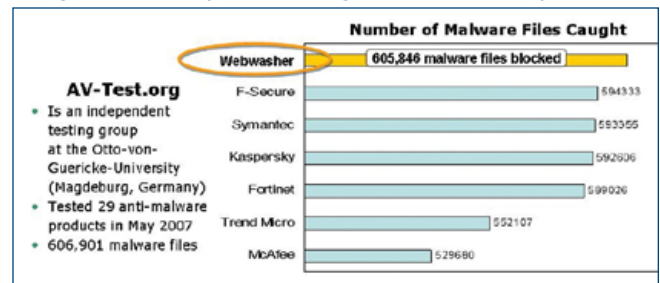


Figure 10: Secure Anti-Malware Engine Layered Security

Advanced Compliance Engine

Protecting from attacks trying to come into the enterprise is only one half of the battle. As specified by Forrester, it’s also important to guard the important information that is required by regulation, privacy concerns intellectual property protection. In addition, it is often required to protect this information in motion through encryption.

Secure Computing’s Advanced Compliance Engine (ACE) provides in-depth protection by using the following techniques to identify, discover and act on risky information as it leaves the enterprise

1. Classification of multiple types of data
2. Auto-learning of protected and unprotected content

¹⁵ *Anti-Malware test performed by AV-Test.org and published on <http://www.eweek.com/article2/0,1895,2023127,00.asp>*

¹⁶ *Source: Stopping the Targeted Attack: Why Comprehensive Malware Protection is Superior to Anti-Virus Signatures for Protecting Your Organization (<http://www.securecomputing.com/Webform.cfm?id=118&ref=ptw1657>)*

3. All variations of the intellectual property including filetype changes and derivative works
4. Application of appropriate action based on policy including content risk and sender
5. Encryption that doesn't rely on end users for triggering, and can be of multiple types and techniques

Secure Computing's advanced compliance technologies add sophistication and flexibility to the built-in dictionaries and lexicons of pattern matching, enabling the discovery of unformatted content as well as intentionally obfuscated data. These advanced technologies include:

- Precise matching
- "Fuzzy" matching
- Document fingerprinting
- Adaptive lexical analysis
- Clustering

For a detailed discussion of how ACE can protect against data leakage, please see our white papers: *Data Leakage, Four Sources of Abuse and Data Leakage, Four Technologies to Protect Content*.¹⁷

Conclusion

With more than 90% of organizations already reporting business value from Web 2.0 adoption, these technologies and applications are here to stay, and destined to become as much a part of our use of the Internet as email and Web browsing. This adoption is creating new security risks for organizations. The previous generation of Web and messaging solutions, which depend on signatures and categorization, have been proven both theoretically and in practice to be insufficient to manage the new risks of the Web 2.0 world and beyond.

Clearly, organizations must deploy new solutions to meet these threats. These new solutions must use reputation- and intent-based techniques to thwart the short-lived, targeted attacks which are becoming the new standard. The principle design requirements for these solutions are well understood and implemented today in commercial products

Secure Computing Secure Web (*Webwasher*) and Secure Mail (*IronMail*) provide proactive, reputation- and intent-based solutions that meet the needs of today's evolving threat landscape, are recognized by third parties and independent test labs as highly effective, and are affordable, secure and reliable.

Next Steps

Check out your domain's reputation with our *Domain Health Check* service. This free report provides you with information on the publicly observed messaging and Web traffic on your domain and any associated net blocks that you provide. The information in this report comes from the Secure Computing TrustedSource service, a global reputation service that tracks messaging and Web activity for every domain on the Internet.

You can also attend a weekly Webinar hosted by Secure Computing to learn more about Secure Web, Secure Mail, and other Secure Computing products. Video demonstrations are also available for Webwasher and IronMail, as well as an extensive library of data sheets and white papers. All of these can be found at www.securecomputing.com.

Lastly, contact Secure Computing's partners for more information on evaluating and purchasing Secure Mail, Secure Web, or other related solutions.

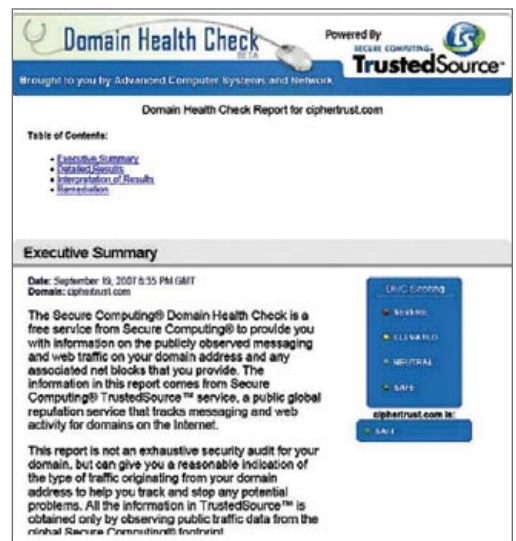


Figure 11: Secure Computing Domain Health Check

¹⁷ Secure Computing white papers: "Data Leakage, Four Sources of Abuse," and "Data Leakage, Four Technologies to Protect Content"